ليـــوا للتعليم
Liwa Education

Data & Cybersecurity Infrastructure Overview

Policy Document

2025-2026

Policy Reference	ET-10
Version	V1
Date of Creation	03112025
Policy Owner	CFO
Date of Approval	05112025
Effective Date	05112025
Date of Review	03112026
Reviewed by	Deputy CEO Director of Schools
Approved by	CEO

A. Rationale

This governance framework establishes the principles and standards required to ensure secure, resilient, and well-managed digital infrastructure and data protection practices across Liwa Education.

As a K–12 education provider operating in Abu Dhabi and Al Ain, Liwa Education is responsible for safeguarding student, staff, and institutional data in compliance with ADEK requirements and applicable UAE regulations.

By establishing clear governance over data management, cybersecurity controls, and digital infrastructure, Liwa Education ensures the protection of confidential information, the continuity of school operations, and the integrity of its digital learning environment.

B. Purpose

- Define group-wide governance standards for data protection, cybersecurity, and digital infrastructure across all Liwa Education campuses.
- Establish minimum security principles that guide the design, management, and monitoring of information systems, networks, and data assets.
- Ensure accountability for cybersecurity risk management and regulatory compliance throughout the organization.

C. Scope

This policy applies to all Liwa Education campuses, departments, and affiliated entities.

It applies to all information systems, networks, cloud services, devices, applications, and data assets used for educational or operational purposes.

It applies to all employees, contractors, third-party vendors, and partners who access or manage Liwa Education systems or data.

D. Policy

1. Governance and Oversight

- The IT Department maintains centralized governance over cybersecurity and data protection standards.
- Each campus implements controls aligned with group standards and maintains secure infrastructure.
- Cybersecurity risks are identified, documented, and escalated where necessary.
- Significant infrastructure or system changes impacting security are reviewed through governance channels before implementation.

2. Network and Infrastructure Security

- All campuses operate protected network environments secured with enterprise-grade perimeter security.
- Network segmentation separates administrative systems, staff networks, student networks, guest access, and critical services.
- Secure communication protocols and encryption are enforced for internal and external data transmission.
- Remote access is controlled through secure authentication mechanisms.
- Firewall security, web filtering, and traffic inspection are centrally managed by the IT Department.
- Requests for access to blocked content must follow formal approval procedures.

3. Identity and Access Management

- Access to systems and data is granted based on role and legitimate operational or educational need.
- Administrative and privileged accounts are secured with enhanced controls, including multi-factor authentication.
- Access rights are reviewed periodically.
- Accounts are disabled promptly when employment or engagement ends.

4. Data Protection and Backup

- Student, safeguarding, HR, and financial data are classified as confidential and protected accordingly.
- Data is protected during transmission and where feasible at rest using encryption.
- Backup solutions are implemented for critical systems and data.
- Backup restoration procedures are periodically tested.
- Data retention and disposal practices comply with regulatory and ADEK requirements.

5. Endpoint and System Security

- Staff and approved student devices accessing institutional systems must comply with approved security controls.
- Device management platforms may be used to enforce configuration standards, deploy applications, and apply restrictions.
- Content filtering and safeguarding controls are implemented where appropriate.
- Systems and applications are maintained with security updates and patches.
- Endpoint protection tools provide threat detection, malware protection, and centralized monitoring.

6. Monitoring, Risk Management and Compliance

- Security monitoring mechanisms detect unauthorized access, suspicious activity, and threats.
- Vulnerabilities and risks are assessed and addressed promptly.
- Campuses support internal cybersecurity reviews and audits when required.
- This policy aligns with ADEK Digital Policy requirements and UAE cybersecurity regulations.
- Implementation of specific cybersecurity technologies may vary by campus and follow the approved phased development roadmap.

E. Roles and Responsibilities

IT Department:

Responsible for defining cybersecurity and infrastructure standards, overseeing implementation, and maintaining technical security controls including firewall protection, endpoint security, device management, and monitoring systems.

Campus Leadership:

Responsible for ensuring compliance with group cybersecurity governance standards at campus level.

Employees and System Users:

Responsible for following approved security practices and reporting suspected security incidents.

Chief Finance Officer (CFO)

Responsible for overseeing the governance of this policy, ensuring alignment with Liwa Education's cybersecurity and data protection standards, and approving updates prior to submission for executive approval.

F. Policy Review and Maintenance

This policy will be reviewed annually or following significant changes in regulatory requirements, cybersecurity risk landscape, or infrastructure strategy.

Updates will be approved in accordance with Liwa Education governance procedures.

Appendix A – Firewall and Network Security Controls

Liwa Education maintains enterprise-grade firewall and network security controls to safeguard institutional infrastructure and internet connectivity across campuses. Firewall and web security policies are centrally managed by the IT Department.

Core security controls include:
- Firewall security policy and traffic inspection
- Network segmentation for staff, student, and guest networks
- Web filtering and category-based access control
- Security exception review procedures
- Network monitoring and threat detection

Firewall security policies enforce differentiated access for staff and student networks. Student networks apply stricter filtering controls designed to block categories of websites considered inappropriate, unsafe, or unrelated to educational activities.

Firewall systems also provide threat protection, intrusion prevention, and encrypted traffic inspection to defend against ransomware, malware, phishing attempts, and other cyber threats.

Appendix B – Apple Education Privacy and Data Protection Controls

Liwa Education utilizes Apple education services including Apple School Manager and Managed Apple IDs to support device management, student access to educational resources, and secure learning environments.

Key privacy protections include:
- Student data remains under the ownership and control of the school
- Apple acts as a data processor on behalf of the school
- Student data is encrypted both in transit and at rest
- Access to student information is limited to authorized personnel based on role

permissions
• Managed Apple IDs restrict purchasing, communications, and non-educational activity

Apple services used within the education environment include:
• Apple School Manager
• Classroom
• Schoolwork
• Shared iPad environments
• iCloud services for managed education accounts

These services operate under strict privacy standards designed to ensure transparency, secure data handling, and protection of student information.

Appendix C – Device Management and Mobile Device Security

Liwa Education implements Mobile Device Management (MDM) solutions to ensure secure configuration, monitoring, and lifecycle management of institutional devices.

Device management capabilities include:
• Deployment and configuration of applications
• Remote troubleshooting and device support
• Device inventory monitoring
• Security policy enforcement
• Remote lock and data wipe capabilities for lost or stolen devices

MDM platforms may also support Bring Your Own Device (BYOD) programs while ensuring separation between personal and institutional data.

Appendix D – Content Filtering and Online Safety

Content filtering technologies are implemented to maintain a safe digital learning environment for students.

Filtering systems may:
- Block harmful or inappropriate websites
- Monitor online activity on school-managed devices
- Detect cyberbullying or unsafe behaviour indicators
- Provide reporting to authorized school staff

These systems support student safeguarding objectives and ensure compliance with digital safety standards required for educational environments.

Appendix E – Endpoint Protection and Antivirus Security

Endpoint protection solutions are deployed across supported staff devices and servers to defend against malware, ransomware, phishing attacks, and other cyber threats.

Core capabilities include:
- Real-time threat detection and blocking
- Scheduled system scanning
- Automatic virus definition updates
- Safe browsing protection
- Quarantine and removal of infected files
- Centralized monitoring and reporting

Endpoint security tools help protect sensitive institutional data and ensure secure operation of digital systems.

Appendix F – Network Access and Authentication Controls

Network access to institutional systems is governed by secure authentication mechanisms and controlled access policies.

Network access management capabilities include:
- User-based authentication for network access
- Role-based permissions and device limits
- Multi-step authentication for staff networks
- Monitoring of connected devices and network activity
- Secure onboarding and offboarding of employee accounts

Access credentials are issued and managed by the IT Department and may be disabled or modified when users change roles or leave the organization.

Policy Owner Department

Education Technology Department

Key Stakeholders		
Policy Owner:	Brian Joaquim Fernandes	Chief Finance Officer
Reviewed by:	Margaret Haynes	Director of Schools
	Kevin Wallis	Deputy CEO
Approved by:	Dr. Shereen Gobran	Chief Executive Officer